Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities	)	GN Docket No. 13-111

COMMENTS OF VERIZON

William H. Johnson
Of Counsel

Gregory M. Romano
Robert G. Morse
1300 I Street, N.W.
Suite 500 East
Washington, DC 20005
(202) 515-2400

Attorneys for Verizon

June 19, 2017

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities	)	GN Docket No. 13-111

COMMENTS OF VERIZON

The rules the Commission adopted in March will enable state and local authorities to deploy and use managed access systems ("MAS") to combat the serious problem of inmates unlawfully using contraband wireless devices in correctional facilities. The most effective approach for the Commission to curb such use is to encourage correctional facilities and wireless licensees to use the new rules to deploy and develop reliable MAS technologies. Encouraging innovation in and widespread deployment of those technologies should largely prevent the use of contraband handsets without harming legitimate wireless device use inside and outside of a correctional facility's premises, including 911 calling.

The new rules are just now going into effect, and the Commission should allow state and local authorities time to procure, negotiate, and deploy new MAS technologies in correctional facilities. If the Commission decides to adopt additional rules at this time, it should ensure that the requirements are carefully balanced and take into account existing technical challenges as well as the potential impact on the public and legitimate users of devices. For example, rather than requiring wireless companies to completely disable contraband devices, the Commission should allow companies to simply terminate or suspend service to those devices. And it should

adopt procedures to provide the same level of confidence and liability protection associated with court orders before carriers are required to terminate service to particular devices. Doing so will protect legitimate users and minimize licensees' liability risk for implementing a correctional facility's request. The Commission also should leave the details of operational issues, such as licensees notifying Contraband Interdiction Systems ("CIS") vendors of network changes, and CIS vendors notifying licensees of impacts on licensees' networks, to contractual arrangements between the parties. Finally, the Commission should not require licensees to implement quiet zone and device-based solutions; licensees cannot realistically deploy them ubiquitously in the near future and they could harm wireless consumers in affected areas.

I. THE STREAMLINED PROCESS IN THE NEW RULES WILL ENABLE CORRECTIONAL FACILITIES TO DEPLOY AND USE MAS SYSTEMS TO ADDRESS UNLAWFUL USE OF CONTRABAND DEVICES.

The new rules adopted in March streamline the notification, negotiation, and approval process for states and localities to deploy and use MAS technologies. Deploying effective MAS technologies should make cell detection and service termination systems unnecessary, while better protecting legitimate users in and near correctional facilities. That is because MAS technologies can assess and allow authorized devices to communicate normally with the commercial wireless network and to allow 911 calling, while blocking transmissions to or from unauthorized devices.

Verizon has already implemented spectrum leasing arrangements for CIS providers in correctional facilities in four states. Through its support of these early efforts, Verizon has already largely standardized its approach to these MAS-based arrangements, including both the

contractual terms and conditions and the technical parameters of spectrum leases.[1] The new streamlined procedures for CIS-related spectrum leasing agreements, and the good faith negotiation duty now imposed on wireless licensees under the Commission's new rules, will facilitate similar arrangements among CIS providers and other licensees in the immediate future. Widespread deployment of MAS networks should thus help quickly curtail the unlawful use of contraband devices in correctional facilities, calling into question the need for detection systems and service termination requirements that risk snaring legitimate users' devices.

II. ANY SERVICE TERMINATION PROCESS SHOULD INCORPORATE QUALITY CONTROL MEASURES TO GIVE LEGITIMATE USERS AND LICENSEES THE SAME PROTECTIONS AS A COURT-BASED APPROACH.

If the Commission decides to move ahead with rules requiring service termination despite the promise of MAS deployment, it must adopt a balanced approach to avoid unnecessary disruption to legitimate users. Use of court orders provides that balanced approach. Court orders work because: a court's evidentiary standards compel the party seeking injunctive action to have a valid factual basis for the request; service providers already have procedures in place that can be adapted to handle requests such as these; and the service provider does not face criminal or civil liability for implementing the request. So if the Commission implements its own process to terminate service to contraband devices, it should replicate these aspects of a court-based approach to best balance public safety needs against the risk of terminating service for legitimate users.

---

[1] *See Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd 2336, ¶¶ 63-64 (2017) ("*Report and Order*" or "*Further Notice*").

A. Quality Control Measures Must Precede Service Termination Requests to Mitigate the Risk of Harm to Legitimate Users.

If the Commission decides that service termination is an appropriate way to address contraband devices, it should supplement the appropriate quality control safeguards proposed in the *Further Notice* to minimize the risk of an erroneous request terminating service to a legitimate user. Eligibility standards for CIS providers and performance standards for cell detection solutions will help ensure that correctional facilities and their vendors deploy and operate their systems per the terms of their spectrum leases and lease agreements, and test the reliability of any cell detection system. But the Commission should also require the presence of, and compliance with, a valid spectrum lease to ensure oversight diligence by the Designated Correctional Facility Official ("DCFO") and its CIS vendor.[2] Spectrum lease terms will limit adverse impact on licensees' legitimate users, but licensees will have only limited (if any) visibility into the CIS provider's operations and practices. So it is critical that the DCFO and its vendor be able to attest they are adhering to those agreed-to lease parameters. And DCFO requests should originate from those state or local government officials with oversight responsibility over the CIS provider vendor's contract and operations. That will ensure accountability by the state or local officials directly responsible for the CIS provider's acts and omissions.[3] A Commission-maintained "master list" of permitted DCFOs also would help mitigate disputes over whether a request is valid.[4]

---

[2] *See id.* ¶¶ 96-98.

[3] *See id.* ¶ 99.

[4] *See id.* ¶ 100.

The *Further Notice* underscores correctly that the contents of a request, including a certification by a DCFO, help drive quality control. The request criteria the Commission proposes make good sense. For example, Verizon agrees that these criteria should include requiring the correctional facility to provide unique device identification information, in particular the device's Mobile Directory Number (MDN) and another identifier such as international mobile subscriber identity (IMSI), Mobile Equipment Identifier (MEID) or International Mobile Equipment Identity (IMEI) if possible, and to certify that: it uses an eligible CIS provider with a validated cell detection system; the CIS provider possesses a spectrum lease in good standing; and it contacted all licensees in the area. But to strike an appropriate balance, the Commission should also apply performance and validation standards to cell detection systems to ensure that termination of detected devices will not ensnare legitimate users that live or commute near correctional facilities.[5]

B. The Commission Should Transmit an Order Directing the Licensee to Terminate Service to a Device.

Quality control measures will help minimize misidentification of handsets as contraband, but may not prevent all misidentification of devices. So the Commission should also ensure that service providers who comply with its rules do not face liability for misidentified handsets simply for implementing a request under the Commission's rules. To avoid that, the Commission staff, not the DCFO, should transmit the request to the licensee's designated point of contact.[6] And that transmittal should include a Commission- or Bureau-level letter order

[5] *See id.* ¶ 100.

[6] *See id.* ¶ 98.

directing the licensee to comply.[7] While Section 303 of the Communications Act gives the Commission considerable regulatory authority in this area, directing a licensee to cease providing service amounts to an injunctive action. An order directing service providers to comply with a DCFO request will thus help provide licensees liability protection commensurate with a judicial process.[8] And doing so will help ensure that licensees can implement the requests expeditiously without any need to second-guess the merits and accuracy of the request.[9]

For those same reasons, a licensee should not be responsible for verifying or investigating the accuracy of a service termination request, as suggested in the *Further Notice*.[10] The *Further Notice* does not clarify what the licensee's "verification" role would entail, or the extent of due diligence required by the licensee. The DCFO and the Commission's underlying quality control and cell detection performance standards, not licensees, should perform this verification function. The licensee's role should at most be limited to confirming that the request is valid on

---

[7] A Bureau letter compelling a party to take such action would be an "Order" for purposes of the Communications Act and the Administrative Procedure Act. *See* 5 U.S.C. § 551(6) (defining an "order" as "the whole or a part of a final disposition, whether affirmative, negative, *injunctive*, or declaratory in form, of an agency in a matter other than rule making but including licensing" (emphasis supplied)); *LDC Telecomms., Inc.*, Notice of Apparent Liability for Forfeiture and Order, 27 FCC Rcd 300, ¶ 5 (EB 2012) ("[t]he Bureau's Letter of Inquiry directed to LDC was a legal order of the Commission requiring LDC to produce the requested documents and information"); *see also Star Wireless, LLC v. FCC*, 522 F.3d 469, 474 (D.C. Cir. 2008) (official interpretation issued by staff on delegated authority, including in a letter, has same force and effect as other Commission actions).

[8] For example, the Stored Communications Act provides that "No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter." 18 U.S.C. § 2703(e).

[9] *See* 47 U.S.C. § 154(i) (Commission may "issue such orders, not inconsistent with this Act, as may be necessary in the execution of its functions.").

[10] *See Further Notice* ¶¶ 106-107.

its face, i.e. that it "is what it purports to be,"[11] and to implementing it if technically possible. But the judgment call of whether to terminate service to a device in these circumstances should rest with correctional facility officials and the Commission.

III. THE COMMISSION SHOULD REQUIRE THAT SERVICE PROVIDERS TERMINATE SERVICE, NOT DISABLE THE DEVICE.

Although service termination may be an appropriate approach, subject to the balancing and safeguards discussed above, the Commission should not adopt the *Further Notice*'s proposal that licensees "completely disable the contraband device itself and render it unusable, not simply terminate service to the device."[12] To remotely and reliably disable appropriate devices would require extensive development by a number of players in the wireless ecosystem. And even once developed, the capability would not address the large embedded base of handsets in the marketplace today. The Commission should instead focus on proven alternatives that licensees can implement more quickly.

A new system to handle service termination requests will require significant but reasonable implementation efforts. For example, to consistently and expeditiously implement a valid service termination request, industry and public safety stakeholders should develop a standardized, common format for qualifying requests. But wireless providers can adapt their existing fraud prevention and law enforcement support systems to process service termination requests without the need to also develop and deploy the new device or network capabilities

---

[11] *Cf. Communications Assistance for Law Enforcement Act*, Report and Order, 14 FCC Rcd 4151, ¶ 34 (1999) (in law enforcement intercept context, to comply with CALEA Section 105 requirements a carrier does not conduct *de novo* review or an intercept request but need only "determine if such authorization is what it purports to be, and whether it can be implemented technically, including that the authorization is sufficiently and accurately detailed to enable the carrier to comply with its terms").

[12] *Further Notice* ¶ 95.

needed to completely disable the device. Terminating or suspending service to a device is an established, common practice for licensees and their customers. Licensees' existing service suspension practices and platforms, and experience with the stolen phones database, should inform any framework the Commission develops.[13] It would also be valuable for qualifying requests to cover all service providers serving the correctional facility's area – not just the user's current network – to minimize inmates' ability to circumvent a request by swapping out SIM cards.

But the ability to fully and remotely "disable" and "re-enable" a handset by disabling or locking it entirely (as is possible for some devices under the wireless industry's efforts to mitigate device theft)[14] is currently limited to certain smartphone models and not available for feature phones and other connected devices. And a licensee cannot disable devices today based on the unique device identifiers visible to the licensee; the disabling capability is instead tied to the user's account with the operating system provider (e.g., iOS or Android). To achieve the *Further Notice*'s proposed requirements, a new disabling capability would be required for all connected devices. That would require significant device and operating system development and network/back end infrastructure changes, as well as the involvement and cooperation of multiple vendors in the ecosystem. And the increasing number of device models offered outside of a licensee's own retail channels could create additional implementation challenges for a service provider-controlled capability. Service providers cannot ensure that devices not sold by service

---

[13] *See, e.g.*, https://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting12414/TAC-MDTP-Report-v1.0-FINAL-TAC-version.pdf, at 34-35, 49-50, 133-34.

[14] *See* https://www.ctia.org/docs/default-source/default-document-library/stolen-phone-commitment-new.pdf.

providers include such capability, or that those devices' disabling capability would be compatible with their networks.

Finally, once the new capability could be available, it still would take years for the embedded base of handsets to drop out of use before this capability could have a meaningful impact. The Commission's and industry's experience in transitioning the embedded base of handsets to E-911 location-capable models illustrates how handset turnover can resist carrier marketing efforts.[15] Rather than rely on this untested approach that would have, at most, a distant impact, the Commission should maintain its focus on other efforts, such as managed access systems and possibly service termination methods, which could more quickly help address the problem of contraband devices.

III. LEASING ARRANGEMENTS SHOULD GOVERN NOTICE OF NETWORK CHANGES AND INTERFERENCE ISSUES.

The *Further Notice* proposes new notification requirements on the use of MAS systems that are best left to contractual negotiations. For example, the *Further Notice* asks whether licensees should provide 30-90 days advance notification to CIS providers of significant network changes, and proposes that CIS operators notify licensees within 24 hours when the former's operations adversely affect the licensee's network.[16] But the Commission already mandates that

---

[15] *See Revision of the Commission's Rules To Ensure Compatibility with Enhanced 911 Emergency Calling Systems*, Fourth Memorandum Opinion and Order, 15 FCC Rcd 17442, ¶ 36 (2000) ("we concur with those commenters that argue that the current schedule [for carriers to reach full penetration of ALI-capable handsets] may have been overly ambitious, in view of consumers that may wish to continue to use their non-ALI capable handsets, even if newer handsets provide location as well as other advanced features").

[16] *Further Notice* ¶¶ 117-121.

licensees and CIS providers negotiate leasing agreements in good faith, and notification provisions such as these, when necessary, are standard in those agreements.[17]

The operational details on which the Commission seeks comment – e.g., the types of network upgrades that warrant advance notice, the duration of that notice, and methods of protecting licensees' proprietary business plans – do not belong in prescriptive rules. Verizon's own experience with CIS operators underscores that the parties have ample incentive to resolve these issues on a timely and reasonable basis in ways that protect both parties' sensitive business plan information. And notice requirements could quickly become obsolete. For example, the emergence of Self-Optimized Networks (SONs) means that many network changes relating to frequency and network use do not need to be, and are not, known in advance. Companies also often use industry-based channels for widespread dissemination of information regarding some significant network changes, obviating the need for a lessee-specific, formal notification process.

IV. OTHER, ALTERNATE SOLUTIONS RAISED IN THE *FURTHER NOTICE* COULD NEGATIVELY AFFECT LEGITIMATE USERS AND ARE UNNECESSARY.

The Commission adopted a technically sound, innovative market-oriented approach to addressing the problem of contraband devices just a few months ago. Service providers are already working with correctional facilities and their CIS providers to enter into spectrum lease agreements and deploy new MAS systems. The Commission should build upon proven solutions deployed in the marketplace, without requiring costly re-engineering of networks and in a manner consistent with the Communications Act's prohibition against jamming devices.

---

[17] *See* 47 C.F.R. § 20.23(a).

With the promise of MAS systems and for the reasons Verizon described in its earlier comments, the Commission should reject a "quiet zone" approach in which licensees are obligated to discontinue service within a geographic area designed by the correctional facility.[18] The construction of new correctional facilities, or an existing correctional facility's authorization for new quiet zone status within licensees' existing coverage areas, would require that wireless providers either re-design their radio access networks or substantially power down their transmitters. Both options would impose significant costs on licensees and adversely affect the reliability of service to consumers. Many correctional facilities are in or near urban and suburban areas and major thoroughfares with established coverage and that are the focus of licensees' ongoing network densification and 5G deployment efforts. This approach would also implicate Section 316 of the Act by modifying a wireless provider's licensed geographic area without an adjudication.[19]

Other quiet zone and "network-based" proposals described in the *Further Notice* would rely on "geo-fencing" capabilities dependent on interplay between the device and the licensee's network. Beacon technology proposals are likewise dependent on the interplay between the handset and beacon devices distributed ubiquitously throughout the correctional facility itself. As the Commission acknowledges, all these proposals, including the so-called "network-based" solutions, are actually dependent on the development of highly accurate *device-level* capabilities.[20] While location-based services continue to improve in accuracy, different location

---

[18] *See Further Notice* ¶ 123; Verizon 2013 Reply Comments at 10-11; CTIA 2013 Reply Comments at 10-11.

[19] *See* 47 U.S.C. § 316(a).

[20] *See Further Notice* ¶ 128.

technologies perform differently in different environments. GPS-based technologies would face challenges in the deep indoor environments of a correctional facility, and it is unlikely that lower-power Wi-Fi-based location technologies that can be used to support or backstop GPS-based solutions are widely available in correctional institutions. Beacon-based solutions are dependent not only on the capabilities of devices and the ability of OEMs to integrate the relevant hardware and software capabilities into their products, but the ubiquity of capable devices (and absence of non-capable devices) among users, and the ubiquitous deployment of beacon devices throughout a correctional facility.

Device-based solutions such as these would thus take years to implement and even longer to meaningfully limit the abuse of contraband handsets. So, for these reasons as well, the Commission should encourage state and local government corrections agencies to focus their resources on MAS-based systems that operate consistent with the new rules.

CONCLUSION

The Commission should encourage state and local governments and wireless service providers to take advantage of the technically sound, innovative market-oriented approach to addressing the problem of contraband devices adopted in the *Report and Order*. Any new requirements, such as service termination, should take a balanced approach that accounts for the interests of legitimate wireless users. As companies and correctional facilities implement these existing capabilities and approaches, the Commission should not impose additional prescriptive

requirements for spectrum lease arrangements, much less the speculative alternate interdiction solutions that would adversely affect legitimate users.

Respectfully submitted,

/s/ *Robert G. Morse*

William H. Johnson
Of Counsel

Gregory M. Romano
Robert G. Morse
1300 I Street, N.W.
Suite 500 East
Washington, DC 20005
(202) 515-2400

Attorneys for Verizon

June 19, 2017